Several Classes of Cyclic and Negacyclic Codes with Distance Optimal

Xianmang He

November 27, 2024

Abstract

The construction of cyclic and negacyclic codes with distances-optimal has been an active topic in coding theory. In this paper, we construct several families of infinite many cyclic and negacyclic distance-optimal codes. Firstly, we devise a family of infinite many binary cyclic codes possessing a minimum distance of 8 and 10, and extend this approach to any even distance $2l(l \geq 2)$. Additionally, we introduce a family of quaternary cyclic codes with a minimum distance of 6. Furthermore, we establish an family of infinite many negacyclic BCH codes over the field $GF(5)$. Notably, all the codes constructed in this paper are distance-optimal.

Index terms: Distance-optimal code, Cyclic code. Negacyclic code, Cyclotomic Coset

1 Introduction

Cyclic codes was introduced by E. Prange in 1957 [1], and have been studied for many years. Cyclic codes, a subclass of linear codes, are subject to an additional constraint: all codewords are cyclic permutations of each other. This property renders cyclic codes highly useful in practical applications, particularly in terms of hardware implementation. Their encoding and decoding can be achieved through Linear Feedback Shift Registers (LFSRs). LFSRs are hardware circuits capable of efficiently generating and detecting cyclic code codewords.

For a prime power $q > 1$, let $\mathbb{F}_q$ be the field with q elements. A linear code $\mathbb{C} \subset \mathbb{F}_q^n$ is cyclic if $\forall(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{C}$, the vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathbb{C}$. A codeword $\mathbf{c}$ in a cyclic code corresponds to a polynomial $\mathbf{c}(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1)$. Every cyclic code corresponds to a principal ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$ and it is generated by a factor $\mathbf{g}$ of $x^n - 1$.

Negacyclic codes were first introduced in 1968 by Berlekamp [2, 3]. A code $\mathbb{C} \subset \mathbb{F}_q^n$ is defined as negacyclic if $\forall(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{C}$, the negacyclic shift $(-c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathbb{C}$. A codeword $\mathbf{c}$ in a negacyclic code can be associated with a polynomial

$\mathbf{C}(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n+1)$. Every negacyclic code constitutes a principal ideal in the ring $\mathbb{F}_q[x]/(x^n+1)$ and then generated by a factor $\mathbf{g}$ of x^n+1.

The Bose-Chaudhuri-Hocquenghem (BCH) codes, a type of cyclic code, were introduced in 1959-1960. For more details, refer to the specified source [4, 5, 6]. Similarly, Reed-Solomon codes, which are also cyclic, were introduced in 1960. Further information can be found in the indicated reference [7].

Whether there exists an infinite family of asymptotically good cyclic codes is a long-standing open problem. Therefore, it is interesting to construct infinite families of explicit cyclic and negacyclic codes with a rate of $\frac{1}{2}$ such that their minimum distances are as large as possible. In this paper, several classes of distance-optimal cyclic codes are constructed explicitly.

2 Preliminaries

In this section, let's first review a few basic definitions, notations and facts.

Definition 2.1 (Hamming Weight) *For a vector* $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ *, its Hamming weight* $wt(\mathbf{a})$ *is the cardinality of its support* $wt(\mathbf{a}) = |supp(\mathbf{a}) : \{i : a_i \neq 0\}|$.

Definition 2.2 (Hamming Distance) *For any two vector* $\forall \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$*, the Hamming distance* $d(\mathbf{a}, \mathbf{b}) = wt(\mathbf{a} - \mathbf{b})$*. Hence,* $\mathbb{F}_q^n$ *is a finite Hamming metric space.*

Definition 2.3 (Minimum Hamming Distance) *For a code* $\mathbb{C} \subset \mathbb{F}_q^n$*, any two different codewords* $\mathbf{a}, \mathbf{b} \in \mathbb{C}$*, its Hamming distance* $d = \min_{\mathbf{a} \neq \mathbf{b}}\{d(\mathbf{a}, \mathbf{b}), \mathbf{a}, \mathbf{b} \in \mathbb{C}\}$.

A q-ary linear code with the length n, the dimension k and the minimum distance d, is denoted by a linear $[n, k]_q$ (or $[n, k, d]_q$) code. Let $\mathbb{C} \subset \mathbb{F}_q^n$ be an $(n, M, d)_q$ code, the weight distribution of $\mathbb{C}$ is $\Sigma_{i=0}^{n} A_i(\mathbb{C}) x^i y^{n-i}$, where $A_i(\mathbb{C})$ is the number of codewords in $\mathbb{C}$ with weight i. We refer to [8, 9, 10] for theory of error-correcting codes. A q-ary code with the length n, cardinality M, and minimum distance d, is denoted by an $(n, M, d)_q$ code. The subcode consisting of codewords whose coordinates at one fixed position are zero, is called a shortening code. It is clear that the shortening code of a linear $[n, k, d]_q$ code is a linear $[n-1, \geq k-1, \geq d]_q$ code. The projection code by deleting one fixed coordinate position is the punctured code. The punctured code of a linear $[n, k, d]_q$ code is a linear $[n-1, k, \geq d-1]_q$ code, if $d \geq 2$.

The sphere packing bound for $(n, M, d)_q$ codes states that the number of codewords is upper bounded by the volume of a Hamming ball of radius $\lfloor \frac{d-1}{2} \rfloor$) in the n-dimensional space over $\mathbb{F}_q$. Specifically, the bound is give by

$$M \cdot V_q(\lfloor \frac{d-1}{2} \rfloor) \leq q^n,$$

where $V_q(r) = 1 + n(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$ represents the volume of a ball with the radius r in the Hamming metric space $\mathbb{F}_q^n$. This is because balls centered

at codewords with the radius $\lfloor \frac{d-1}{2} \rfloor$ must be disjoints to maintain a minimum distance d between any two codewords, see [8, 9, 10]. Chen [11] provides a new upper bound on the linear code size related to the code weight distribution in amazement.

Let $\mathbb{C} \subset \mathbb{F}_q^n$ be an $(n, M, d)_q$ code, if there does not exist an $(n, M, d+1)_q$ code, then $\mathbb{C}$ is referred to as a distance-optimal code. Some distance-optimal codes are optimal with respect to the sphere packing bound, indicating that $\mathbb{C}$ is an $(n, M, d)_q$ code and $M \cdot V_q(\lfloor \frac{d}{2} \rfloor) > q^n$. Various bounds on the minimum distances of cyclic codes, such as the Hartmann-Tzeng bound and the Roos bound, have been proposed and utilized to construct effective cyclic codes, as detailed in [10, Chapter 6] and [8, Chapter 4]. The Boston bounds and their generalizations for cyclic codes are presented in [12, 13].

Let n be a positive integer satisfying $\gcd(n, q) = 1$, and $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z} = \{0, 1, \ldots, n-1\}$ be the residue class module n.

Definition 2.4 (q-cyclotomic coset) *A subset C_i of $\mathbf{Z}_n$ is called a q-cyclotomic coset if*

$$C_i = \{i, iq, \ldots, iq^{l-1}\},$$

where $i \in \mathbf{Z}_n$ is fixed and l is the smallest positive integer such that $iq^l \equiv i \ mod \ n$.

It is evident that q-cyclotomic cosets are associated with the irreducible factors of $x^n - 1$ in $\mathbb{F}_q[x]$. The generator polynomial of a cyclic code with the length n is the product of several irreducible factors of $x^n - 1$. Let β be the n-th primitive root of the smallest extension field of $\mathbb{F}_q$. Then, the defining set of a q-ary cyclic code of length n generated by $\mathbf{g}$ is given by:

$$\mathbf{T_g} = \{i : \mathbf{g}(\beta^i) = 0\}.$$

Thus, the defining set of a cyclic code is the union of several disjoint q-cyclotomic cosets. In light of the BCH lower bound, if the defining set contains $\delta - 1$ consecutive elements, then the minimum distance of the cyclic code is at least δ. The value δ is referred to as the designed distance. For numerous results on BCH codes, we refer to recent literature [4, 5, 6, 8, 9, 10, 14, 15].

Let $\mathbf{Z}_{2n} = \mathbf{Z}/2n\mathbf{Z} = \{0, 1, \ldots, 2n-1\}$. Similar to cyclic codes, A cyclotomic coset $C_i \in \mathbf{Z}_{2n}$ is termed odd if it contains only odd integers. It is evident that odd cyclotomic cosets in $\mathbf{Z}_{2n}$ correspond to the irreducible factors of x^{n+1} in $\mathbb{F}_q[x]$. The generator polynomial of a negacyclic code is the product of several irreducible factors of x^{n+1}. The defining set of a negacyclic code generated by g is given by:

$$\mathbf{T_g} = \{i : \mathbf{g}(\beta^i) = 0\}.$$

Thus, the defining set of a negacyclic code is the union of several disjoint odd cyclotomic cosets in $\mathbf{Z}_{2n}$. If the defining set of a negacyclic code contains $\delta - 1$ consecutive odd integers, the minimum distance of this negacyclic code is at least δ. This is known as the BCH bound for negacyclic codes, and δ is the designed distance, as discussed in [2, 3].

2.1 Recent Results and Our Contribution

[16] reports the first infinite family of binary distance-optimal BCH codes with the minimum distance 8. Some optimal ternary cyclic codes with the length $3^m - 1$ and minimum distance four and five were constructed in [17]. Distance-optimal codes with minimum distance four and six were constructed in [18, 19, 20, 21]. It is clear that negacyclic codes have been less studied, and several families of distance-optimal ternary negacyclic codes with small minimum distances have been constructed in [22]. Two infinite classes of ternary negacyclic self-dual codes with a square-root-like lower bound on their minimum distances are presented in [23]. There are only few distance-optimal codes with minimum distance six reported in the literature, see [20] and [24, Theorem 9]. [25] construct several families of q-ary self-dual negacyclic codes of lengths n with their minimum distances larger than or equal to $n^{\frac{1}{2}}$ for various lengths n and any given odd prime power q. Chen[26] construct several classes of cyclic and negacyclic codes with distance-optimal, which provides a new approach for constructing distance optimal codes, paving the way for the construction of this paper.

Our contributions. The main contributions of this paper are summarized as follow.

1. we construct infinitely many families of distance-optimal binary BCH code with minimum distance 8 and 10. Building on this approach, we can extend this approach to any even distance $2\ell(\ell \geq 2)$. Consequently, we can construct an infinite many families of distance-optimal BCH code: $[2^m - 1, 2^m - 1 - (\ell - 1) \cdot m - 1, 2\ell]_2$.

2. we introduce a family of quaternary cyclic codes with a minimum distance 6.

3. we establish an family of infinite many negacyclic BCH codes over the field $GF(5)$ with a minimum distance 4.

3 Distance-Optimal Codes

In this section, we give several infinite class of new distance-optimal cyclic and negacyclic codes with distance optimal.

3.1 Distance-optimal Binary Cyclic Codes with Distance 8

Let $n = 2^m - 1$, where $m \geq 6$ is an positive integer. Since $2^m = 1 \bmod n$, 2-cyclotomic coset C_1 in $\mathbf{Z}_n$ has m elements. Besides, the 2-cyclotomic coset C_3, C_5 all have m elements by the fact that $3 \cdot 2^m \equiv 3 \bmod n$, $5 \cdot 2^m = 5 \bmod n$. Therefore, the defining set

$$\mathbf{T} = C_0 \bigcup C_1 \bigcup C_3 \bigcup C_5 \tag{1}$$

has $3m + 1$ elements. Then an infinite family of $[2^m - 1, 2^m - 1 - 3m - 1]_2$ codes is constructed, $m = 6, 7, \ldots$. We have the following result.

Theorem 3.1 *Let $n = 2^m - 1, m \geq 6$ be an positive integer. Then an family of distance-optimal cyclic $[2^m - 1, 2^m - 1 - 3m - 1, 8]_2$ codes is constructed.*

Proof. *The first conclusion follows from the BCH bound, since the consecutive integers $0, 1, 2, 3, 4, 5, 6$ are in the defining set $\mathbf{T}$. The second conclusion follows from the sphere packing bound: $M \cdot V_2(4) \geq 2^n$, where $k = 2^m - 1 - 3m - 1, M = 2^k$. Observe that the volume of the ball of the radius 4 in the hamming metric space $\mathbf{F}_2$ fullfills $V_2(4) = 1 + n + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} > 2^{3m+1}$, when $m \geq 6$.*

We notice that $V_2(4) = 1 + n + \binom{n}{2} + \binom{n}{3} + \binom{n}{4}$ can be expanded as follows: $\frac{24n}{24} + \frac{12n(n-1)}{24} + \frac{4n(n-1)(n-2)}{24} + \frac{n(n-1)(n-2)(n-3)}{24}$.

With some similar items are merged, and finally we have:

$$V_2(4) = \frac{n^4 - 2n^3 + 11n^2 + 14n + 24}{24},$$

Substitute $n = 2^m - 1$ into polynomial $V_2(4)$, after a series of calculations, the following expression is obtained:

$$V_2(4) = \frac{2^{4m} - 6 \cdot 2^{3m} + 23 \cdot 2^{2m} - 18 \cdot 2^m + 34}{24}.$$

Note that $23 \cdot 2^{2m} - 18 \cdot 2^m + 34$ is greater than 0, therefore, we need to prove $2^{4m} - 6 \cdot 2^{3m} > 24 \cdot 2^{3m+1}$. In the end, if $m \geq 6$, then $2^m \cdot 2^{3m} - 6 \cdot 2^{3m} \geq (64 - 6) \cdot 2^{3m} > 48 \cdot 2^{3m}$. Therefore, the codes in this family are distance-optimal.

The first three codes of this family have parameters $[63, 44, 8]_2, [127, 105, 8]_2, [255, 230, 8]_2$. Further, we can get $[255 - t, 230 - t, 8]_2$ shortening codes for $t = 0, \ldots, 181$, from this cyclic $[255, 230, 8]_2$ code. Even though these 181 binary linear codes have the same parameters as best known ones in [27], the best known linear $[74, 59, 8]_2$ code in [27] was constructed from a stored generator matrix, while our construction is simple and effective.

Let the length of the binary cyclic code be $n = \frac{2^m - 1}{\lambda}$, where λ is a divisor of $2^m - 1$. Then each 2-cyclotomic coset in $\mathbf{Z}_n$ has at most m elements. The defining set

$$\mathbf{T} = C_0 \bigcup C_1 \bigcup C_3 \bigcup C_5$$

has at most $3m + 1$ elements. An infinite family of cyclic $[\frac{2^m - 1}{\lambda}, \geq \frac{2^m - 1}{\lambda} - (3m + 1)]_2$ codes is constructed, Therefore we have the following result.

Theorem 3.2 *If λ is a divisor of $2^m - 1$ and satisfies $m > \log_2(48\lambda^4 + 2\lambda + 4)$, then a binary distance-optimal cyclic $[\frac{2^m - 1}{\lambda}, \geq \frac{2^m - 1}{\lambda} - 3m - 1, 8]_2$ code is constructed, when m is sufficiently large.*

Proof. *There are* $0, 1, 2, 3, 4, 5, 6$ *are in the defining set* $\mathbf{T}$*. Then* $d \geq 8$ *from the BCH bound. From the condition we get*

$$V_2(4) = \frac{2^{4m} - 2(2+\lambda)2^{3m} + (2+\lambda)(3+5\lambda)2^{2m} - 2(2+3\lambda-7\lambda^3)2^m + (1+2\lambda+11\lambda^2-14\lambda^3+24\lambda^4)}{24\lambda^4}$$

Hence,

$$V_2(4) > \frac{2^{4m} - 2(2+\lambda)2^{3m}}{24\lambda^4} > 2^{3m+1},$$

when m *is a sufficiently large positive integer, then the minimum distance is 8 and this family of codes are distance-optimal.*

Notice that if λ is fixed positive integer, $m_1, m_2, \ldots,$ are positive integers, going to the infinity, such that $\lambda | 2^{m_i} - 1$, then we always have the following infinite family of distance-optimal binary cyclic codes.

Corollary 3.1 If λ is a fixed positive integer, $m_1 < m_2 < m_3 <, \ldots,$ is a sequence of positive integers such that $\lambda | 2^{m_i} - 1$, then a binary distance-optimal cyclic $[\frac{2^{m_i}-1}{\lambda}, \geq \frac{2^{m_i}-1}{\lambda} - 3m_i - 1, 8]_2$ code is constructed, when m_i is sufficiently large.

For instance, we derive an infinite family of distance-optimal cyclic $[\frac{2^m-1}{7}, \geq \frac{2^m-1}{7} - 3m - 1, 8]_2$ codes. In fact, as long as $2^m > 7^4 \cdot 48 + 18$, that is $m \geq 17$, the sphere packing bound can be guaranteed that $V_2(4) \geq 2^{3m+1}$, therefore, a multitude of such distance-optimal binary cyclic codes with novel parameters can be constructed similarly, expanding ways of the construction for binary optimal-distance cyclic codes.

3.2 Distance Optimal Binary Cyclic Codes With Minimum Distance 10

Let $n = 2^m - 1$, where $m \geq 8$ is an positive integer. It is clear that each 2-cyclotomic coset in $\mathbf{Z}_n$ has exactly m elements since $2^m = 1 \bmod n$. Therefore, the defining set

$$\mathbf{T} = C_0 \bigcup C_1 \bigcup C_3 \bigcup C_5 \bigcup C_7 \tag{2}$$

has at $1 + 4m$ elements. Let $\mathbf{C}$ be a cyclic code generated by $\mathbf{T}$. Then $\mathbf{C}$ is a $[2^m, 2^m - 4m - 2]_2$ cyclic codes. We have the following result.

Theorem 3.3 Let $m \geq 8$ be an positive integer. Then an infinite family of distance-optimal cyclic $[2^m - 1, 2^m - 4m - 2, 10]_2$ codes is constructed.

Proof. *Since* $0, 1, 2, 3, 4, 5, 6, 7, 8$ *are in the defining set* $\mathbf{T}$*, then* $d \geq 10$ *from the BCH bound. Observe that the volume of the ball of the radius* 5 *in the Hamming metric space* $\mathbf{F}_2^n$ *satisfies that* $V_2(5) = 1 + n + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5} = \frac{n^5 - 9n^4 + 15n^3 - 7n^2 + 104n + 120}{120}$.

Let $m \geq 8$*,* $n = 2^m - 1$*, then we have* $V_2(5) = \frac{2^{5m} - 14 \cdot 2^{4m} + 61 \cdot 2^{3m} - 116 \cdot 2^{2m} + 204 \cdot 2^m - 25}{120}$*. Note that it can be easily verified that* $61 \cdot 2^{3m} - 116 \cdot 2^{2m} + 204 \cdot 2^m - 25 > 0$*.* $2^5 m - 14 \cdot 2^{4m} \geq (256 - 14) \cdot 2^{4m} > 120 \cdot 2^{4m+1}$*. Therefore, the codes in this family are distance-optimal.*

The first code of this family have parameters $[255, 222, 10]_2$. From [27], the current $[255, 222, 10]_2$ is obtained by shortening of $[257, 224, 10]_2$, and $[257, 224, 10]$ is obtained by adding a parity check bit to $[256, 224, 9]_2$.

Similar to the Theorem 3.2, we have the following binary infinite family of distance-optimal cyclic codes.

Theorem 3.4 *If λ is a divisor of $2^m - 1$, then a binary distance-optimal cyclic $[\frac{2^m-1}{\lambda}, \geq \frac{2^m-1}{\lambda} - 4m - 1, 10]_2$ code is constructed, when m is sufficiently large.*

From the above construction process, as long as m is sufficiently large, we can construct a family of binary distance-optimal cyclic code and minimum distance $d = 2\ell(\ell \geq 2)$: $[2^m - 1, 2^m - 1 - (k-1) \cdot m - 1, 2\ell]_2$, and the defining set $\mathbf{T}$ is defined by:

$$\mathbf{T} = C_0 \bigcup C_1 \bigcup \cdots \bigcup C_{2\ell-3} \tag{3}$$

Theorem 3.5 *Let m be a positive integer and sufficient large, then an infinite family of distance-optimal cyclic code with the parameters $[2^m - 1, 2^m - 1 - (\ell - 1) \cdot m - 1, 2\ell]_2$ is constructed.*

Proof. *Since $0, 1, 2, 3, 4, 5, 6, 7, \cdots, 2k-2$ are in the defining set $\mathbf{T}$, then $d \geq 2\ell$ from the BCH bound.*

Observe that the volume of the ball of the radius k in the Hamming metric space $\mathbb{F}_2^n$ satisfies that $V_2(\ell) = 1 + n + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \cdots + \binom{n}{\ell}$.

For any $\ell(\ell \leq \frac{n}{2})$, the specific expression is not easy to write directly, but we know that the first two terms must be $\frac{n^\ell - a_1 \cdot n^{\ell-1} + g(\ell)}{\ell!}$, where $g(\ell) > 0$ and a_1 is an integer greater than 0. Then substitute $n = 2^m - 1$, resulting in $V_2(\ell) > \frac{2^{m\ell} - a_2 \cdot 2^{m(\ell-1)}}{\ell!}, (a_2 > 0)$. Now, we need to prove that $V_2(\ell) > 2^{(m-1)\ell+1}$, It is obvious that as long as m is large enough that $2^m > (a_2 + 2 \cdot \ell!)$, then $2^{m\ell} > (a_2 + 2 \cdot \ell!) \cdot 2^{m(\ell-1)}$.

3.3 Distance-optimal Quaternary Cyclic Codes With Distance 6

Let $n = 4^m - 1$, where $m \geq 3$ is a positive integer. Note that $4^m = 1 \bmod n$. Each 4-coset contains m elements. Let the defining set be

$$\mathbf{T} = C_0 \bigcup C_1 \bigcup C_2 \bigcup C_3. \tag{4}$$

We get an infinite family of distance-optimal quaternary cyclic codes with minimum distance 6.

Theorem 3.6 *Let $n = 4^m - 1$, and m be a positive integer satisfying $m \geq 3$. The codes defined above is a family of distance-optimal cyclic $[4^m - 1, 4^m - 3m - 2, 6]_4$ codes.*

Proof. *The consecutive integers 0, 1, 2, 3, 4 are in the defining set* $\mathbf{T}$*. From the BCH bound, the minimum distance of codes in the above family is at least* 6*. Note that the volume of the ball of the radius 3 in the hamming metric space* $\mathbf{F}_4$ *satisfying*

$$V_4(3) = 1 + (q-1)n + (q-1)^2 \cdot \frac{n(n-1)}{2} + (q-1)^3 \cdot \frac{n(n-1)(n-2)}{6} \geq q^{3m+1}.$$

Then these codes are distance-optimal with respect to the sphere packing bounds.

Then, we have $V_4(3) = \frac{64n^3-165n^2+123n+6}{6} = \frac{64\cdot 4^{3m}-357\cdot 4^{2m}+645\cdot 4^m-276}{6} = 4^{3m+1} + \frac{46\cdot 4^{3m}-357\cdot 4^{2m}+645\cdot 4^m-276}{6}$. *This is easy to verify that* $V_4(3) > 4^{3m+1}$*, when* $m \geq 3$.

Notice these distance-optimal quaternary cyclic codes can be compared with distance-optimal quaternary codes in [21]. The first two codes in this family have parameters $[63, 53, 6]_4$, $[255, 242, 6]_4$. The shortening of the $[255, 242, 6]_4$ code is a $[255-t, 242-t, 6]_4$ linear code, where $0 \leq t \leq 184$. Although these 184 binary linear codes have the same parameters as best known ones in [27], and the best known linear $[71, 58, 6]_4$ code in [27] was constructed from a stored generator matrix again.

It is natural to question whether an infinite family of distance-optimal codes can be constructed for any given ratio λ with code length $n = \frac{4^m-1}{\lambda}$. However, this is not possible. For instance, when $\lambda = 3$, the sphere packing bound is not satisfied. By substituting $n = \frac{4^m-1}{3}$ into the polynomial $P(n) = \frac{64n^3-165n^2+123n+6}{6}$, we derive an expression $(\frac{64\cdot 4^{3m}-687\cdot 4^{2m}+3289\cdot 4^m-1504}{162})$ that is evidently less than 4^{3m+1}. This indicates that constructing an infinite family of distance-optimal codes for all values of λ is not feasible.

3.4 Distance-optimal Negacyclic Codes over $\mathbf{F}_5$ With Distance 4

Let $n = \frac{5^m-1}{2}$, where $m \geq 2$ is a positive integer. $5^m = 1 \bmod 2n$, each 5-cyclotomic coset in $\mathbf{Z}_{2n}$ has exactly m elements. Define the defining set

$$\mathbf{T} = C_1 \bigcup C_3.$$

Theorem 3.7 *Let* n *and* $\mathbf{T}$ *be defined as above. An infinite family of distance-optimal negacyclic* $[\frac{5^m-1}{2}, \frac{5^m-1}{2} - 2m, 4]_5$ *codes is constructed.*

Proof. *The consecutive integers 1,3,5 are in the defining set* $\mathbf{T}$*. The distance conclusion follows from the BCH bound for negacyclic codes. The second conclusion follows from the sphere packing bound:*

$V_5(2) = 1 + 4n + 8n(n-1) = 2 \cdot 5^{2m} - 14 \cdot 5^m + 5 > 5^{2m} + 5^m \cdot 5^m - 14 \cdot 5^m > 5^{2m}$*. when* $m \geq 2$.

The two codes is $[62, 56, 4]_5, [312, 304, 4]_5$. By the shortening, the optimal $[130-t, 122-t, 4]_5$ $(0 \leq t \leq 3)$ codes can also be obtained from $[312, 304, 4]_5$.

Let us make a discussion about the feasibility of constructing an infinite family of distance-optimal codes for any integer λ, where the length n is defined as $\frac{5^m}{\lambda}$. However,

the answer to this feasibility is still negative. Specifically, in the case where λ equals 3, the sphere packing bound is violated. By substituting $n = \frac{5^m-1}{3}$ into the polynomial $P(n) = 1 + 4n + 8n(n-1)$, we obtain the result $\frac{8\cdot 5^{2m}-60\cdot 5^m+29}{9}$, which is less than 5^{2m}. This calculation illustrates that it is not possible to construct such an infinite family of distance-optimal codes for all values of λ.

4 Conclusion

In this paper, we presents the development of several infinite families of cyclic and negacyclic codes that are distance-optimal, a topic of significant interest in coding theory. We construct several families of infinite cyclic and negacyclic distance-optimal codes, including binary cyclic codes with minimum distances of 8 and 10, extendable to any even distance 2ℓ ($\ell \geq 2$). Additionally, we introduce a family of quaternary cyclic codes with a minimum distance of 6, and an infinite family of negacyclic BCH codes over the field $GF(5)$ with a minimum distance of 4. All the codes presented in the paper are proven to be distance-optimal, contributing to the theoretical advancements and practical applications in coding theory.

References

[1] E. Prange, *Cyclic Error-Correcting Codes in Two Symbols.* Cambridge, MA :Air Force Cambridge Research Center, 1957.

[2] E. R. Berlekamp, "Negacyclic codes for the lee metric," in *Proc. Conf. Combin. Math. and Appl.*, 1966, pp. 298–316. [Online]. Available: https://api.semanticscholar.org/CorpusID:123314145

[3] T. Blackford, "Negacyclic duadic codes," *Finite Fields and Their Applications*, vol. 14, no. 4, pp. 930–943, 2008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1071579708000191

[4] R. Bose and D. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, no. 1, pp. 68–79, 1960. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0019995860902874

[5] ——, "Further results on error correcting binary group codes," *Information and Control*, vol. 3, no. 3, pp. 279–290, 1960. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0019995860908706

[6] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres (Paris)*, vol. 2, pp. 147–156, 1959.

[7] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960. [Online]. Available: https://doi.org/10.1137/0108018

[8] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[9] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes,3rd Edition*. North-Holland Mathematical Library, Amsterdam, 1977.

[10] J. H. van Lint, *Introduction to the coding theory, Third and Expanded Edition*. vol. 86, Springer, Berlin, 1999.

[11] H. Chen and C. Xie, "A new upper bound for linear codes and vanishing partial weight distributions," *IEEE Transactions on Information Theory*, vol. 70, no. 12, pp. 8713–8722, 2024.

[12] N. Boston, "Bounding minimum distances of cyclic codes using algebraic geometry," *Electronic Notes in Discrete Mathematics*, vol. 6, pp. 385–394, 2001, wCC2001, International Workshop on Coding and Cryptography. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1571065304001908

[13] A. Zeh, A. Wachter-Zeh, and S. V. Bezzateev, "Decoding cyclic codes up to a new bound on the minimum distance," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3951–3960, 2012.

[14] C. Ding and C. Li, "Bch cyclic codes," *Discrete Mathematics*, vol. 347, no. 5, p. 113918, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0012365X24000499

[15] S. Noguchi, X.-N. Lu, M. Jimbo, and Y. Miao, "Bch codes with minimum distance proportional to code length," *SIAM Journal on Discrete Mathematics*, vol. 35, no. 1, pp. 179–193, 2021.

[16] C. Xie, H. Chen, and C. Yuan, "Explicit cyclic and quasi-cyclic codes with optimal, best known parameters, and large relative minimum distances," *IEEE Transactions on Information Theory*, vol. 70, no. 12, pp. 8688–8697, 2024.

[17] N. Li, C. Li, T. Helleseth, C. Ding, and X. Tang, "Optimal ternary cyclic codes with minimum distance four and five," *Finite Fields and Their Applications*, vol. 30, pp. 100–120, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1071579714000835

[18] J. Yuan, C. Carlet, and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 712–717, 2006.

[19] C. Ding and T. Helleseth, "Optimal ternary cyclic codes from monomials," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5898–5904, 2013.

[20] Z. Heng, C. Ding, and W. Wang, "Optimal binary linear codes from maximal arcs," *IEEE Transactions on Information Theory*, vol. 66, no. 9, pp. 5387–5394, 2020.

[21] Z. Heng, Q. Wang, and C. Ding, "Two families of optimal linear codes and their subfield codes," *IEEE Transactions on Information Theory*, vol. 66, no. 11, pp. 6872–6883, 2020.

[22] Z. Sun and C. Ding, "Several families of ternary negacyclic codes and their duals," *IEEE Trans. Inf. Theor.*, vol. 70, no. 5, p. 3226–3241, Jan. 2024. [Online]. Available: https://doi.org/10.1109/TIT.2024.3349996

[23] T. Chen, Z. Sun, C. Xie, H. Chen, and C. Ding, "Two classes of constacyclic codes with a square-root-like lower bound," *IEEE Transactions on Information Theory*, vol. 70, no. 12, pp. 8734–8745, 2024.

[24] X. Wang, D. Zheng, and C. Ding, "Some punctured codes of several families of binary linear codes," *IEEE Transactions on Information Theory*, vol. 67, no. 8, pp. 5133–5148, 2021.

[25] C. Xie, H. Chen, C. Ding, and Z. Sun, "Self-dual negacyclic codes with variable lengths and square-root-like lower bounds on the minimum distances," *IEEE Transactions on Information Theory*, vol. 70, no. 7, pp. 4879–4888, 2024.

[26] H. Chen and Y. Wu, "Cyclic and negacyclic codes with optimal and best known minimum distances," *IEEE Transactions on Information Theory*, vol. 70, no. 12, pp. 8628–8635, 2024.

[27] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," *Online available at http://www.codetables.de.*